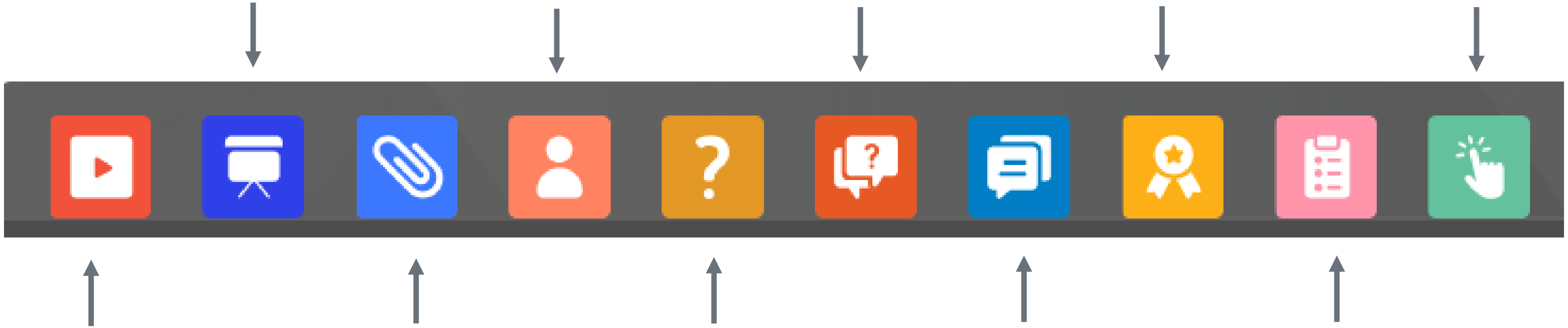
CompTIA Network+ N10-009 TTT Session 8:

Title

July 18, 2024

CompTIA

@TeachCompTIA #PenTestPlusTTT



Multimedia

Slides

Today’s Resources

Bios

ON24 Help

Q&A

Group Chat

Certificate of Attendance

Survey

Call to Action

Network+ Team

Instructor:
Don Tilley
Cybersecurity Instructor,
Program Director
Access Computer Training
dontilley130@gmail.com

Instructor:
Brian Ford
Technical Instructor
CompTIA
BFord@comptia.global

CIN

CompTIA

INSTRUCTOR NETWORK

The CompTIA Instructor Network (CIN) is a worldwide community for instructors who provide CompTIA certification training.

Benefits of being a community member include:

- Communicate and collaborate with CompTIA staff and other instructors.
- Access resources for students to understand the value of getting certified.
- Receive complimentary training and tools from CompTIA to enrich your classroom.
- Become proficient at teaching CompTIA standards.
- Share best practices and resources with each other.

Google Play

App Store

https://cin.comptia.org

PARTNERSUMMIT 24

JULY 30TH

sync

CompTIA INSTRUCTOR NETWORK

CIN

TRAIN THE TRAINER

WORKSHOPS

CompTIA Tech+

CIN

CompTIA Network+

CompTIA A+

Join us for the morning session from 9:00 a.m. to 12:00 p.m. or the afternoon session from 1:00 p.m. to 4:00 p.m.
Each session is $99.00.
Lunch and refreshments provided

Workshop sessions:

1. Get In Sync with the new CompTIA Tech+ FC0-U71
2. Teaching CompTIA Network+ N10-009 with the new CertMaster Perform
3. Tools for teaching CompTIA A+ 1100 Series

Each session provides:

- Access to official CompTIA content for the course
- Instructor led training and labs
- Certificate of completion provided at the end of session.

Hyatt Regency Atlanta
July 31 – August 1
Register today: https://connect.comptia.org/partnersummit/home

CompTIA

If a bad organizational culture eats ethics for breakfast, then will AI steal your lunch money?

What: One-hour webinar investigating current industry AI trends
When: Thursday July 25th 10:00 a.m. CST
Where: ON24
Who: James Stanger, Chief Technology Evangelist
Register: https://bit.ly/CINPulse-AITrends

@TeachCompTIA

Network+ N10-009 TTT Session Outline

Date	Topic
✓ 06/20/2024	Introduction and Network Topologies
✓ 06/25/2024	Cabling and Physical Installations
✓ 06/27/2024	Configuring Interfaces and Switches
✓ 07/02/2024	Configuring Network Addressing
✓ 07/09/2024	Configuring Routing and Advanced Switching
✓ 07/11/2024	Network Security
✓ 07/16/2024	Network Security (Continued)
✓ 07/18/2024	Wireless Networking
07/23/2024	Troubleshooting and Management
07/25/2024	Emerging Technologies and Trends

CONFIGURING WIRELESS NETWORKS

Learning Objectives

1. Summarize wireless standards.

2. Install and configure secure wireless networks.

3. Troubleshoot wireless networks.

WIRELESS CONCEPTS AND STANDARDS

802.11 Wireless Standards

- Commonly known as Wi-Fi
- Established by the Electrical and Electronics Engineers (IEEE)
- Defines how radio waves communicate over distances
- Ensures compatibility between wireless devices

802.11 Characteristics

- **Physical Layer**
  - Encodes data into radio signals with various modulation
- **Media Access Control (MAC)**
  - Uses CSMA/CA for efficient transmission and to
- **Topologies**
  - Primarily a logical star
  - Centered around an Access Point (AP) connecting
- **Evolution**
  - 1 Mbps in the initial standard
- **Wi-Fi Alliance**
  - Certifies products for standard adherence and device compatibility

802.11a

Frequency Band	Operates in the 5 GHz band Avoids the crowded 2.4 GHz band used by many household devices
Data Rate	Nominal data rate of up to 54 Mbps
Technology	Uses Orthogonal Frequency-Division Multiplexing (OFDM) for efficient data transmission
Pros and Cons	Less prone to interference Shorter range compared to technologies operating in the 2.4 GHz band

802.11b/g

•802.11b

- **Frequency Band**
  - Remains in the 2.4 GHz band
- **Data Rate**
  - Increases to a nominal 11 Mbps
- **Technology**
  - Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) for signal encoding
- **Channel Overlap**
  - Potential for co-channel interference due to overlapping channels

•802.11g

- **Compatibility**
  - Backward support for 802.11b while offering increased data rates
- **Frequency Band**
  - Uses the 2.4 GHz band with the same channel layout as 802.11b
- **Data Rate**
  - Offers a nominal data rate of 54 Mbps using OFDM

802.11n

•Frequency Bands

- Supports both 2.4 GHz and 5 GHz bands
- Accommodates wider channel bandwidth
- Reduced interference

•Technology Enhancements

- Multiple Input Multiple Output (MIMO) and Channel Bonding significantly increases bandwidth and reliability
- Multiple antennae send and receive up to four separate data streams, enhancing signal reliability and range
- Combines two adjacent 20 MHz channels into a single 40 MHz channel for increased data rates

•Data Rate

- Achieves up to 72 Mbps per stream
- Potential rates up to 600 Mbps under optimum conditions

Wi-Fi 5 (802.11ac)

Frequency Band

Operates exclusively on the 5 GHz band

Throughput

Up to Gigabit speeds with 80/160 MHz channel bonding

Spatial Streams

Supports up to 8 spatial streams for enhanced data rates

Modulation

Uses denser modulation at close ranges for higher data throughput

Marketing Labels

Devices marketed using AC values like AC5300 (combined throughput capacities)

Multiuser MIMO

MU-MIMO Introduction

Enhances network efficiency

Allows simultaneous multiple user access

DL MU-MIMO

Multiple antennae AP sends data to multiple stations at once

Wi-Fi Generations

Wi-Fi 5 and 6 support parallel station communications, extending up to 8 stations

Benefits

Better bandwidth and network efficiency

Improved performance

Supports more devices in crowded areas

Cellular Technologies

Feature	2G/3G	4G (LTE/LTE-A)	5G
Peak Data Rate	2G: Up to 384 Kbps 3G: Up to 2 Mbps	LTE: Up to 150 Mbps LTE-A: Up to 300 Mbps	Up to 20 Gbps
Technology Base	2G: Digital voice and SMS 3G: Mobile internet	High-speed mobile Internet	Ultra-high-speed internet, IoT, massive MIMO
Spectrum Use	Limited band use	Efficient use of spectrum	Uses a broad spectrum, low to high bands (sub-1 GHz to 40 GHz)
Typical Use Case	Voice calls, basic internet	Streaming, gaming, HD video	Streaming in 4K/8K, AR/VR, smart cities, autonomous vehicles

Activity: Fill in the Blank

- The ___________ GHz band is used by many household appliances.
- The 802.11 ___________ incorporates MIMO and channel bonding to increase bandwidth and reliability
- ___________ prioritizes connection to 5/6 GHz bands over 2.4 GHz bands.

802.11 Review

Which 802.11 standard introduced MIMO technology and channel bonding? a) 802.11a b) 802.11g c) 802.11n d) 802.11ac

What is the primary frequency band used by 802.11ac (Wi-Fi 5)? a) 2.4 GHz b) 5 GHz c) 6 GHz d) 60 GHz

Game: "Guess the Standard" I'll describe a feature, and you guess which Wi-Fi standard it belongs to:

1. "I introduced MIMO technology and can use both 2.4 GHz and 5 GHz bands."
2. "I operate only in the 5 GHz band and introduced MU-MIMO for downlink."
3. "I'm the latest standard that can use 2.4 GHz, 5 GHz, and potentially 6 GHz bands."

ENTERPRISE WIRELESS NETWORK DESIGN

Wireless Local Area Network (WLAN)

Wireless Local Area Network (WLAN)

Devices communicate over a wireless signal

Uses a network name or Service Set Identifier (SSID) for connection

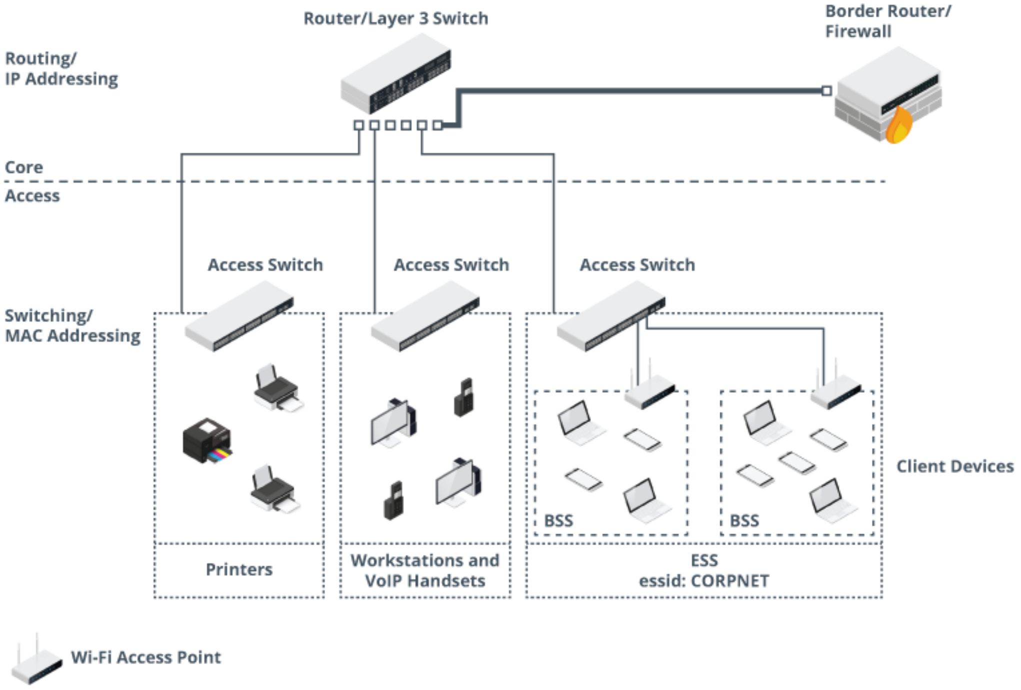
Infrastructure Mode

Access Point (AP) mediates communications

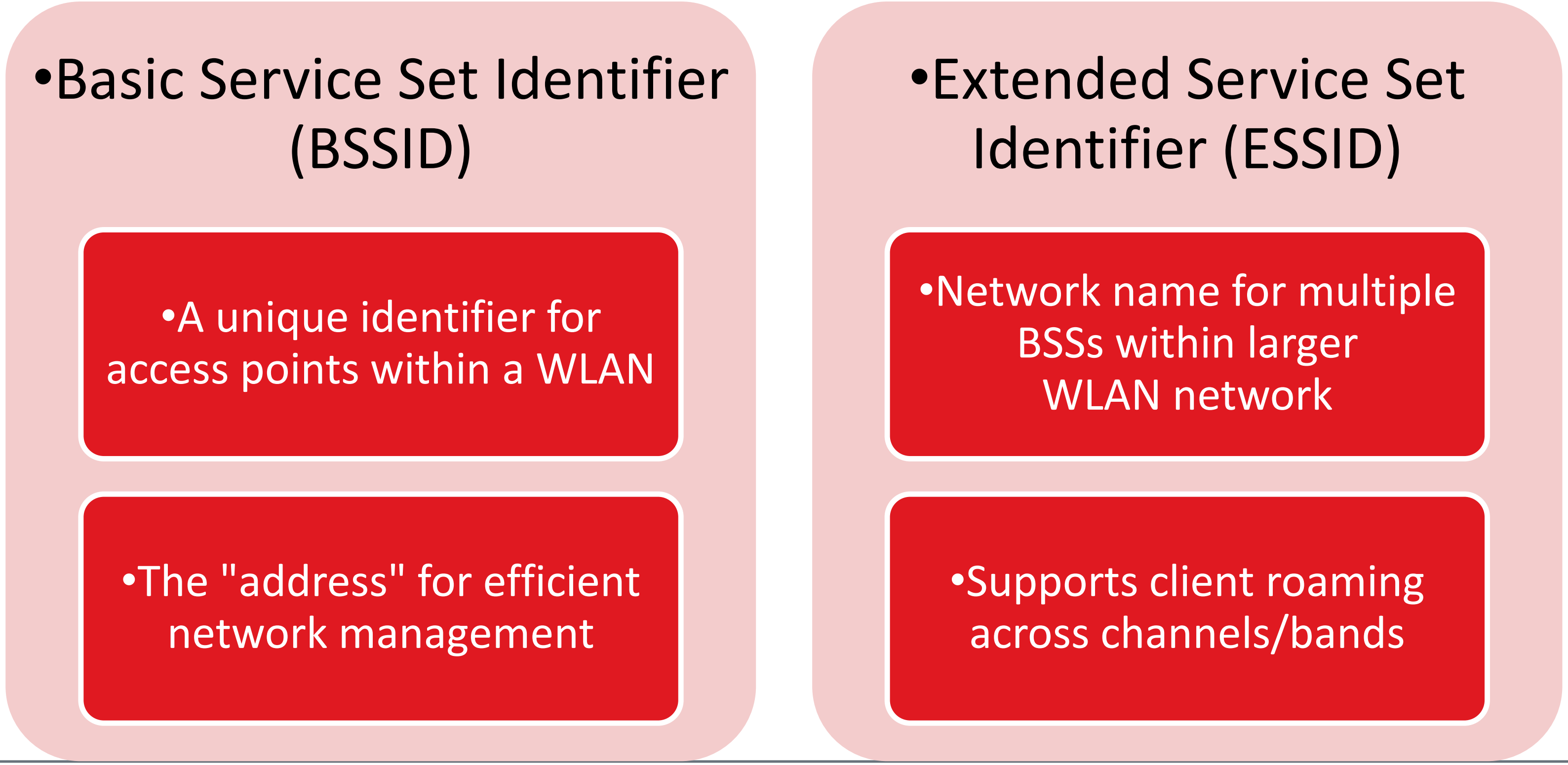
Forms a logical star topology

AP supports multiple BSSs on different bands with unique/shared SSIDs

WLAN Example



BSSID and ESSID



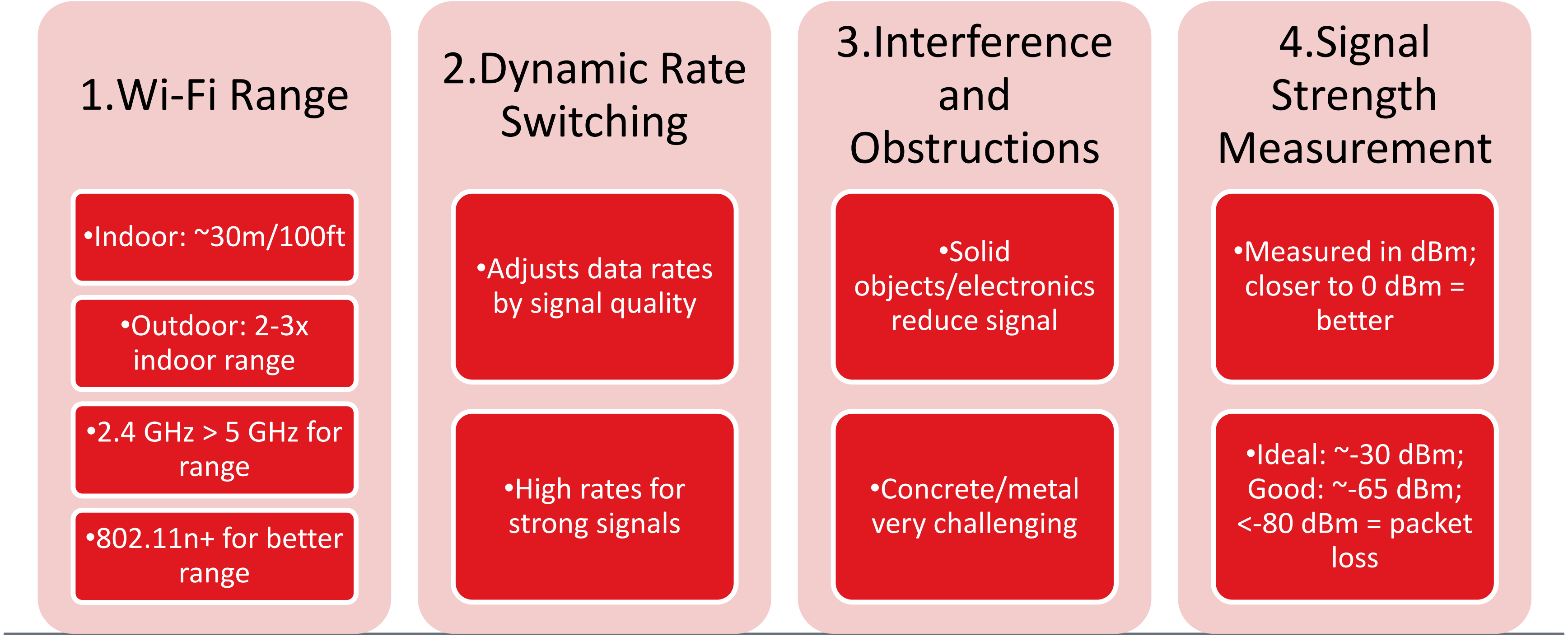
- Basic Service Set Identifier (BSSID)
  - A unique identifier for access points within a WLAN
  - The "address" for efficient network management

- Extended Service Set Identifier (ESSID)
  - Network name for multiple BSSs within larger WLAN network
  - Supports client roaming across channels/bands

Think About It

- Do you notice a difference in speed or performance based on where you are in comparison to the wireless access point?
- What seems to impact your connection?
- How do you fix the issue?

Range and Signal Strength



1.Wi-Fi Range

- Indoor: ~30m/100ft
- Outdoor: 2-3x indoor range
- 2.4 GHz > 5 GHz for range
- 802.11n+ for better range

2.Dynamic Rate Switching

- Adjusts data rates by signal quality
- High rates for strong signals

3.Interference and Obstructions

- Solid objects/electronics reduce signal
- Concrete/metal very challenging

4.Signal Strength Measurement

- Measured in dBm; closer to 0 dBm = better
- Ideal: ~-30 dBm; Good: ~-65 dBm; <-80 dBm = packet loss

Wireless Survey

Definition

- Also known as a WLAN or RF site survey
- Wireless network planning for optimal coverage, bandwidth, and quality of service

Purpose

- Determine the optimal placement of wireless access points
- Identify potential interference sources

Process

- Physical site inspection
- Signal strength measurement
- Data analysis for network planning

Wireless Roaming

Definition	Seamless device connection across APs without disconnects
Extended Service Area (ESA)	Network of APs with the same ESSID and security settings
Seamless Transition	Devices reassociate with new APs based on signal strength, potentially needing reauthentication
Challenges	Needs balance in signal quality assessment and reassociation rate

SSID Broadcast and Beacon Frame Essentials

SSID Broadcast

Facilitates connection to WLAN by advertising its presence

Configurable to enhance security by suppressing broadcast

Beacon Frames

Special frames that carry essential network information like SSID/ESSID, BSSID, and security protocols

Broadcast interval adjustable for network performance

Wireless Distribution System (WDS)

•Purpose

- Creates a wireless network where cabling is impractical

•Configuration Requirements

- Matching SSID, channel, and security settings across APs
- Base station (wired) and remote stations (wireless extension)

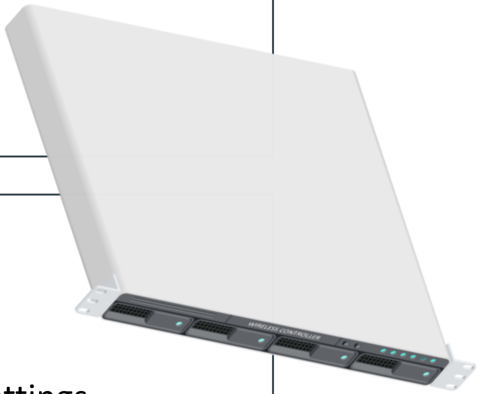
•Vendor Considerations

- Same-manufacturer APs may offer better compatibility and performance

Wireless Controllers

Wireless Controllers

- Manage and monitor multiple APs
- Simplify network configuration
- Prevent individual AP errors
- Offer a comprehensive view of network performance



Functions

- Central management
- Supports up to 1,500 APs and 20,000 clients at once
- Serves as a central point for switching and routing
- Automatically configures SSID, channel, and security settings
- Assigns clients to separate VLANs
- Regulates station numbers per VLAN to minimize broadcast traffic

Antennas

Omnidirectional Antennas

Radiates and receives signals in all directions equally

Wide area coverage: Ideal for spreading the signal across large spaces (ceiling-mounted)

Unidirectional Antennas

Focuses signal on a specific direction

Point-to-point communications, extending signals to remote areas

Provides increased signal strength in the focused area, requires precise alignment

Dual-Polarized Antennas

Transmits and receives signals in multiple orientations

Supports mobile devices well, adaptable to various device orientations

Ensures robust signal quality for devices in different positions

Comparison of Wireless Network Types

•Ad Hoc Topology (IBSS)

- •Peer-to-peer network setup
- •No access point required
- •Small workgroups or single-device connectivity
- •Not scalable for large implementations
- •Modern Windows versions may use Wi-Fi Direct instead

•Mesh Topology (WMN)

- •Nodes discover and peer, forming a Mesh Basic Service Set (MBSS)
- •Routing protocols (HWMP) for path discovery and forwarding
- •Scalable, suitable for IoT networks
- •Stations don't need to be in direct radio range of each other

•Point to Point

- •Direct logical and physical connection between 2 devices
- •Often used to bridge two locations without cables
- •Uses highly directional antennas like dish or Yagi
- •Configured in bridge mode for inter-office connectivity

Activity: What is it?

Antenna that radiates and receives signals in all directions equally

General coverage, suitable for environments where the signal needs to be spread across a wide area

Offers wide coverage, best mounted on ceilings to optimize reach

3
5

Enterprise Wireless Network Design Review

What does ESSID stand for in wireless networking? a) Extended Service Set Identifier b) Enterprise Security System Identifier c) Enhanced Signal Strength Identifier d) External Service Set Identifier

Which of the following best describes the function of a wireless controller? a) Encrypts all wireless traffic b) Manages and monitors multiple access points c) Boosts wireless signal strength d) Filters malicious websites

Game: "Wireless Network Puzzle" Match the following terms with their descriptions:

1. BSSID
2. ESSID
3. Heat Map
4. Wireless Controller

- A. Manages multiple access points centrally B. Unique identifier for an access point C. Visual representation of signal strength D. Network name allowing roaming across multiple access points

WIRELESS SECURITY

Wi-Fi Protected Access 2 (WPA2)

Background

WPA2 is the second generation (2004) of Wi-Fi security protocols

Significantly improved upon WEP and WPA protocols

Encryption Strength

Relies on shared encryption key for all network connected devices

Provides robust protection against common Wi-Fi attacks

Security Protocols

Uses the Advanced Encryption Standard (AES) for data protection

Remains susceptible to interception and other attacks

Wi-Fi Protected Access 3 (WPA3)

Background

- Introduced in 2018 to address the limitations of WPA2

1.Individualized Data Encryption

- Implements individualized data encryption for each device

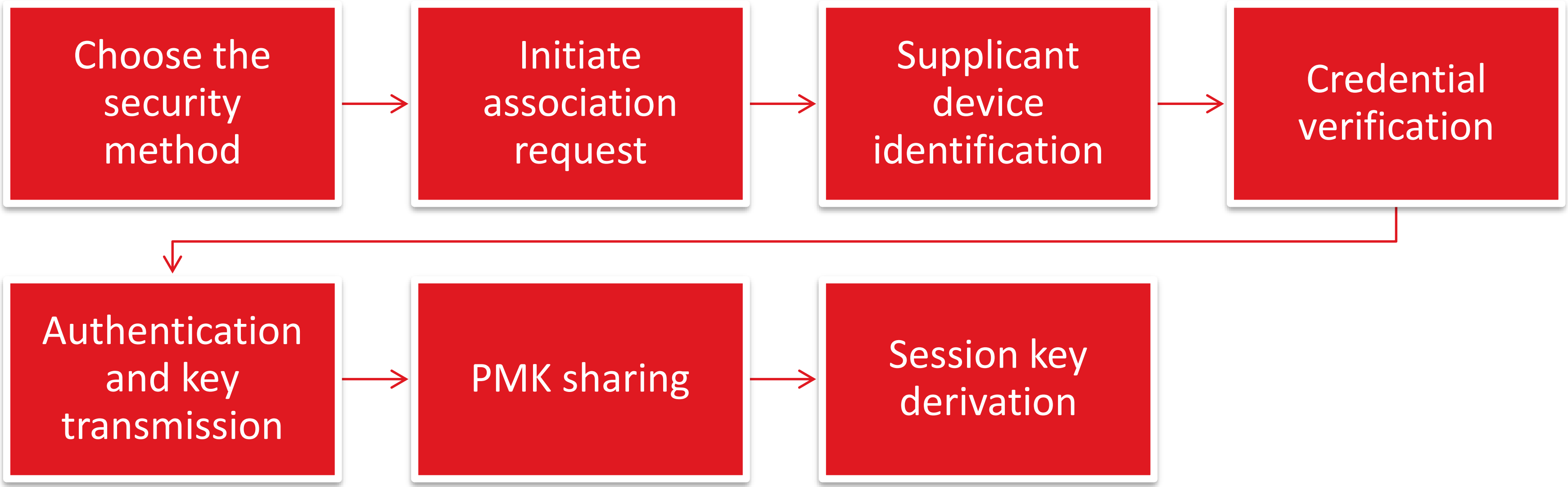
1.Password Protection

- WPA3 makes password cracking much harder
- Attackers must interact with your Wi-Fi for every password guess, making brute force attacks almost impossible

1.Forward Secrecy

- Supports forward secrecy
- If an attacker learns your password later, they can’t decrypt previously captured data—only newly captured data

Enterprise Authentication


Choose the security method
Initiate association request
Supplicant device identification
Credential verification
Authentication and key transmission
PMK sharing
Session key derivation

Guest Networks

Defined	Offer separate access for visitors and traffic isolated from the main network
Benefits	Enhanced Security: Segregating guest user access from internal resources
Accessibility	Simplify connection for guests while maintaining network integrity
Implementation	Separate SSIDs: Distinct from the main network for easy identification Restricted Access: Limits to Internet only (no entry to local servers/sensitive data)

Issues with BYOD

Compatibility & Support

- Complex connectivity across devices/OS
- Ensuring seamless network functionality

Security Concerns

- Varied device security levels
- Unpatched devices as threats
- Limited IT control
- Insider threats
- Data vulnerability

Risk Mitigation

- Implement EMM suites
- Use corporate workspaces
- Enforce security policies
- Segregate corporate/ personal data

Rogue Access Points

Definition

Evil twin: fraudulent Wi-Fi AP mimicking a legitimate network

Users unknowingly connect, allowing attackers to intercept data

How They Work

Rogue APs deceive users by appearing genuine

Attackers capture login details, track connections, install malware

Mitigation

Regularly scan for rogue access points

Educate users about risks; avoid connecting to suspicious networks

Deauthentication Attacks

Definition

Disrupt connections between users and Wi-Fi access points

Attackers force devices to lose access and then reconnect to a network they control

Purpose

Disrupt communication

Attackers track connections, capture data, trick users into installing rogue programs

Detection and Prevention

Monitor network traffic for unusual deauthentication patterns

Implement strong encryption and authentication mechanisms

Evil Twin Network

Definition

Fraudulent Wi-Fi APs lure users into connecting to them instead of legitimate ones

Steal personal data, insert malware, or compromise devices

Function

Attackers set up fake Wi-Fi access points

Users unknowingly connect, thinking it's a legitimate network

Identification

Be cautious in public places with open Wi-Fi networks

Verify network names and use VPNs for added security

Activity: Two Truths and a Lie

- WPA2 uses the Advanced Encryption Standard (AES) for data protection

- WPA2 supports forward secrecy

- WPA2 relies on a shared encryption key for all devices connected to the network

4
7

Wireless Security Review

Which of the following is a key improvement in WPA3 over WPA2? a) Use of AES encryption b) Support for TKIP c) Individualized data encryption for each device d) Implementation of WEP

What is the primary purpose of a captive portal in a guest network? a) To increase network speed b) To require users to authenticate through a web page c) To encrypt all network traffic d) To block all external websites

Game: "Wireless Security True or False" Answer True or False to the following statements:

1. WPA3 uses the same encryption method for all devices on the network.
2. A captive portal is often used to secure guest Wi-Fi networks.
3. Rogue access points are official Wi-Fi hotspots set up by the IT department.
4. BYOD policies always improve network security.

WIRELESS TROUBLESHOOTING

Wireless Performance Assessment

2.Important Metrics

- Bit Rate
- Throughput

3.Understanding RF Attenuation

- Signal degradation with distance governed by the inverse-square rule
- Impact of distance and interference on signal strength measured in dB

4.Concepts in Wireless Connectivity

- Signal-to-Noise Ratio (SNR)
- Optimal SNR Margins

5.Tools for Assessment

- Wi-Fi Analyzers: real-time signal and noise measurements
- Dedicated Wi-Fi Tester Hardware: comprehensive network analysis

Insufficient Wireless Coverage Issues

Definition

Areas with no/poor Wi-Fi signal strength

Results in connectivity issues within a facility

Causes

Signal blockage due to physical obstacles

Greater than optimal distance from access points

Electronic interference from nearby devices

Insufficient Wireless Coverage Solutions

•Extending Coverage	• Install more access points • Use range extenders or wireless bridges
•Antenna Optimization	• Site surveys for ideal placement • Appropriate antenna types
•Power Adjustment	• Calibrate AP transmit power to match weakest client device
•Considerations	• Compatibility with client device wireless standards • Operational frequency bands (optimal performance)
•Goal	• Enhance signal reach/quality • Ensure effective wireless communication

Channel Overlap Issues

Channel Overlap

Occurs with close access points using similar frequencies

Causes interference and reduces network performance

Types of Overlap

Co-channel Interference (CCI): Devices compete
for the same channel

Adjacent Channel Interference (ACI): Devices on overlapping channels slow communication

Channel Overlap Solutions

Design Strategies

Limit channel use to 50% or less for no ACI

Maintain 25 MHz spacing between channels for no ACI

Optimal 2.4 GHz channels: 1, 6, 11

Power Adjustments

Lower AP power to reduce interference

Avoid maximum power to prevent one-way communication problems

Interference Issues

CCI & ACI

Multiple devices on same or close frequencies

Physical Blocks

Walls, furniture, people

Bounce signals, lowering strength and causing issues

EMI

Devices in same frequency (microwaves, Bluetooth)

Disrupts signals

Interference Solutions

Solutions

Place AP strategically to dodge physical blocks and boost signal

Change frequency or channel to cut CCI/ACI

Spectrum Tools

Use to find and fix electromagnetic interference for better signal

Roaming and Disassociation Issues

•Roaming Challenges

- **Sticky Clients**: Fail to switch APs for better connectivity
- **Flapping Clients**: Frequently switching between APs
- **Roaming Standards**: Lack of support for 802.11k, 802.11r, 802.11v affects seamless roaming

•Client Disassociation

- Result from roaming, interference, incompatibility, or malicious attacks
- Exploit unencrypted management frames (denial of service or network compromise)

•Mitigation Strategies

- AP association times/ event logs analysis
- AP placement and power settings for balanced coverage
- Security measures to detect and prevent spoofing attacks

Overcapacity Issues

1.Definition of Overcapacity

- Too many devices attempt to connect to single AP
- Leads to network congestion

•Impact on Performance

- Bandwidth saturation
- Slow speeds or unreliable connections for users

•Common Causes

- High density of client devices in a limited area
- Single AP bearing too many connections beyond capacity

•Effects of Device Saturation

- Includes degraded service, slower web browsing
- Potential bottlenecks moving upstream to the WAN

Overcapacity Solutions

- **Strategic AP Placement**
  - Distribute multiple APs to spread out client device connections evenly.
- **Client Limit Configuration**
  - Set a maximum number of devices that can connect to each AP to prevent overloading
- **Use of Traffic Shaping Tools**
  - Implement traffic shapers to manage bandwidth allocation and prioritize essential services
- **Dynamic Channel Assignment**
  - Use technology to dynamically adjust channels and reduce interference and overuse
- **Continuous Monitoring and Management**
  - Employ enterprise Wi-Fi solutions with advanced diagnostics to identify and mitigate overcapacity issues proactively

Wireless Troubleshooting Review

What does RF attenuation primarily cause in wireless networks? a) Increased network speed b) Better signal quality c) Signal degradation over distance d) Improved network security

Which of the following is NOT a common cause of wireless interference? a) Physical obstacles like walls b) Other electronic devices operating on similar frequencies c) Using WPA3 encryption d) Overlapping wireless channels

Game: "Wireless Trouble Matcher" Match the problem with its likely cause:

1. Slow internet in certain rooms
2. Devices keep disconnecting and reconnecting
3. Wi-Fi works well until the microwave is used
4. Slower speeds when many people are online

- A. Electromagnetic interference B. Overcapacity C. Insufficient coverage D. Roaming issues

Summary

- Define **network requirements**
- **Survey site** with floor plan & Wi-Fi analyzer
- **Determine AP range** for chosen technology
- **Test installation**: size, security, functionality (real-world conditions)

Chat Question

Discussion question asked to the group.

Answer in the chat window and let's share.

Discussion time: Please type your questions in chat

- Questions over content.
- Share you experience.
- What would you like to see different moving forward?

Let’s keep the conversation going in the CompTIA Instructor Forum: https://cin.comptia.org